SOLICITATION/CONTRACT/ORDER FOR COMMERCIAL ITEMS
OFFEROR TO COMPLETE BLOCKS 12, 17, 23, 24, & 30.

1. REQUISITION NUMBER
A21296903

PAGES 1 OF (1) PAGE(S)

2. CONTRACT NO.
GS06F0643Z

3. AWARD/EFFECTIVE DATE
08/15/2017

4. ORDER NUMBER
GSQ1117BJ0044

5. SOLICITATION NUMBER

6. SOLICITATION ISSUE DATE

7. FOR SOLICITATION INFORMATION CALL:

a. NAME

b. TELEPHONE NUMBER *(No Collect Calls)*

8. OFFER DUE DATE/ LOCAL TIME

9. ISSUED BY
GSA Region 11
Reva Hutchinson
301 7th Street, SW Room 6109
Washington DC,
DC
20407-0000
United States
(202) 708-8100

10. THIS ACQUISITION IS
□ UNRESTRICTED
□ SET ASIDE: % FOR
□ SMALL BUSINESS
HUBZONE SMALL BUSINESS
□ 8(A)
NAICS: SIC:
SIZE STANDARD:

11. DELIVERY FOR FOB DESTINATION UNLESS BLOCK IS MARKED
Destination

12. DISCOUNT TERMS
NET 30 DAYS / 0.00 % 0 DAYS / 0.00 % 0 DAYS

□ 13a. THIS CONTRACT IS A RATED ORDER UNDER DPAS (15 CFR 700)

13b. RATING

14. METHOD OF SOLICITATION
RFP

15. DELIVER TO
(b) (4) [redacted]
1401 Constitution Avenue NW
Room 5029
Washington, DC 20230
United States
202-482-4018

16. ADMINISTERED BY
Reva Hutchinson (202) 708-8100

17a. CONTRACTOR/ OFFEROR
(b) (4) [redacted]
CRITERION SYSTEMS, INC.
8330 BOONE BLVD STE 400
VIENNA, VA 221822626
United States
703-942-5800

18a. PAYMENT WILL BE MADE BY

General Services Administration (FUND)
The contractor shall follow these Invoice Submission Instructions. The contractor shall submit invoices electronically by logging into the ASSIST portal (https://portal.fas.gsa.gov), navigating to the appropriate order, and creating the invoice for that order. For additional assistance contact the ASSIST Helpdesk at 877-472-4877. Do NOT submit any invoices directly to the GSA Finance Center (neither by mail nor via electronic submission).

17b. □ CHECK IF REMITTANCE IS DIFFERENT AND PUT SUCH ADDRESS IN OFFER

18b. SUBMIT INVOICES TO ADDRESS SHOWN IN BLOCK 18a UNLESS BLOCK BELOW IS CHECKED

19. ITEM NO	20. SCHEDULE OF SUPPLIES/SERVICES	21. QUANTITY	22. UNIT	23. UNIT PRICE	24. AMOUNT
ITEM NO.	TASK ITEM DESCRIPTION		PREVIOUS MOD AMT	MOD CHANGE AMT	NEW MOD AMT
0001	Base Period Firm Fixed Price CLINs		$0.00	(b) (4) [redacted]	[redacted]
0002	Base Period Labor Hour CLINs		$0.00	[redacted]	[redacted]
0003	Base Period ODC CLIN		$0.00	[redacted]	[redacted]
0004	Base Period Travel		$0.00	[redacted]	[redacted]
0005	Base Period CAF		$0.00	[redacted]	[redacted]

This award is in support of the Department of Commerce to provide IT Support Services. Criterion System's tech[redacted] 2017, revised June 9, 2017, submitted in response to solicitation ID11160043 are accepted as to all items.

The base period of performance is August 15, 2017 through January 14, 2018. The total period of performance is as follows:

Base Period: 8/15/17 - 1/14/18 (b) (4) [redacted]
Option Year One: 1/15/18 - 1/14/19 (b) (4) [redacted]
Option Year Two: 1/15/19 - 1/14/20
Option Year Three: 1/15/20 - 1/14/2
Option Year Four: 1/15/21 - 1/14/22

Total Task Order Value (b) (4) [redacted]

Funds are obligated to the base period as follows:

CLIN 0001 Tasks 1-8 & 12 (b) (4) [redacted]
CLIN 0002 Task 9-11 & 13
CLIN 0003 ODCs (b) (4) [redacted]
CLIN 0004 Travel
CLIN 0005 Contract Access Fee (b) (4) [redacted]

Total Base Period obligated amoun (b) (4) [redacted]

NOTE: Optional Tasks 9,10 and 13 will be funded, exercised and awarded for the base period. In accordance with Section B.8 of the task order, the period of performance start date for theses services will be 10/15/17 - 1/14/18 unless otherwise agreed to by both parties.

NOTE: The Government is not committed to exercise Optional Tasks during Option Periods 1-4. If the option(s) is exercised by the Government, it will be accomplished via a unilateral modification. The contractor shall not invoice against Optional Tasks unless authorized by the Contracting Officer via a written modification to the task order.

25. ACCOUNTING AND APPROPRIATION DATA 285F.Q11FA000.AA20.25.AF151.H08...			26. TOTAL AWARD AMOUNT *(For Govt. Use Only)* (b) (4)	
□ 27a. SOLICITATION INCORPORATES BY REFERENCE FAR 52.212-1, 52.212-4. FAR 52.212-3 and 52.212-5 ARE ATTACHED. ADDENDA N ATTACHED. ☑ 27b. CONTRACT/PURCHASE ORDER INCORPORATES BY REFERENCE FAR 52.212-4. FAR 52.212-5 IS ATTACHED. ADDENDAN ATTACHED.				
28. CONTRACTOR IS NOT REQUIRED TO SIGN THIS DOCUMENT AND RETURN COPIES TO ISSUING OFFICE. □ CONTRACTOR AGREES TO FURNISH AND DELIVER ALL ITEMS SET FORTH OR OTHERWISE IDENTIFIED ABOVE AND ON ANY ADDITIONAL SHEETS SUBJECT TO THE TERMS AND CONDITIONS SPECIFIED HEREIN.		29. AWARD OF CONTRACT: REFERENCE ID11160043 OFFER DATE 5/9/2017. YOUR OFFER ON SOLICITATION (BLOCK 5) INCLUDING ANY ADDITIONS OR CHANGES WHICH ARE SET FORTH HEREIN, IS ACCEPTED AS TO ITEMS:		
30a. SIGNATURE OF OFFEROR/CONTRACTOR		31a. UNITED STATES OF AMERICA *(SIGNATURE OF CONTRACTING OFFICER)* Reva Hutchinson		
30b. NAME AND TITLE OF SIGNER *(Type or print)*	30c. DATE SIGNED	31b. NAME OF CONTRACTING OFFICER *(Type or print)* Reva Hutchinson (202) 708-8100		31c. DATE SIGNED 8/14/2017
32a. QUANTITY IN COLUMN 21 HAS BEEN		32b. SIGNATURE OF AUTHORIZED GOVT. REPRESENTATIVE		32c. DATE
32d. PRINTED NAME AND TITLE OF AUTHORIZED GOVERNMENT REPRESENTATIVE		32f. TELEPHONE NUMBER OF AUTHORIZED GOVERNMENT REPRESENTATIVE		
32e. MAILING ADDRESS OF AUTHORIZED GOVERNMENT REPRESENTATIVE		32g. E-MAIL OF AUTHORIZED GOVERNMENT REPRESENTATIVE		
33. SHIP NUMBER	34. VOUCHER NUMBER	35. AMOUNT VERIFIED CORRECT FOR	36. PAYMENT	
37. CHECK NUMBER		38. S/R ACCOUNT NUMBER	39. S/R VOUCHER NUMBER	40. PAID BY
41a. I CERTIFY THIS ACCOUNT IS CORRECT AND PROPER FOR PAYMENT		42a. RECEIVED BY *(Print)*		
41b. SIGNATURE AND TITLE OF CERTIFYING OFFICER GSA Finance Customer Support 816-926-7287	41c. DATE	42b. RECEIVED AT *(Location)*		
		42c. DATE REC'D *(YY/MM/DD)*	42d. TOTAL CONTAINERS	
AUTHORIZED FOR LOCAL REPRODUCTION		SEE REVERSE SIDE FOR OMB CONTROL NUMBER AND PAPERWORK BURDEN STATEMENT	**STANDARD FORM 1449** (REV. 4-2002) Prescribed by GSA - FAR (48 CFR) 53.212	

SECTION C – DESCRIPTION/SPECIFICATIONS/STATEMENT OF WORK

C.1 PURPOSE

Within the OCIO, the Office of IT Services operates the computer and telecommunications network and security infrastructure at the Herbert C. Hoover building (HCHB). DOC's headquarters is located at 1401 Constitution Avenue, Washington, DC, 20230. The HCHB network infrastructure (HCHBNet) provides data, voice, WiFi/wireless, and emergency broadcast services to several Operating Units that reside within DOC headquarters. Additional services include security monitoring, analysis, and policy enforcement of the network. The Public Address (PA) system support is also provided to the non-renovated sections of the building and is part of this task order. The renovated sections are supported by a fire alarm system supported by GSA via Building Management that is not part of this task order. Voice, data and other IT services are also offered to limited users in the Ronald Reagan Building. The primary purpose of this task order is to provide ongoing operation and maintenance (O&M) of HCHBNet and to enhance the overall service delivery model for the infrastructure.

This task order will also support HCHB renovation. DOC and the GSA Public Building Service are renovating HCHB on a 15 to 20 year schedule. As renovations continue, DOC will require the Contractor to operate, maintain, replace, and upgrade the cable plant, servers, and related HCHBNet components as part of building renovation. This includes supporting cable plant moves, adds and changes (MACs) in the newly renovated spaces as well as cable plant, IT, and phone MACs for work related to office requirements.

In addition, this task order will provide ancillary information technology (IT) support and engineering services for HCHBNet users and applications that run on or over HCHBNet. Additionally, operations and maintenance of network components that extend beyond HCHB, including the internet, MPLS and TLS services; and DOC OCIO and operating units' network, system engineering and system enhancement projects.

Furthermore, this task order will provide service desk support for the DOC/Office of the Secretary and three other OUs, including Economic Development Administration (EDA), Economic and Statistics Administration (ESA) and Minority Business Development Administration (MBDA).

Lastly, this task order will provide Audio Visual and VTC O&M and live webcast streaming support. This includes support to ensure the audio visual and video teleconferencing systems are operating at an optimal level and live webcast events are conducted and supported.

C.1.2 BACKGROUND

The DOC OCIO is responsible for the development and implementation of the agency's Enterprise Architecture, spanning IT systems and technical services across the department's Operating Units (OU) (International Trade Administration, National Telecommunications and Information Administration, Economic Development Administration, etc.) and staff offices (Chief Financial Officer, etc.). In this role, the OCIO is supported by the departments

Enterprise Architecture Advisory Group and other stakeholders. Departmental adherence to Government-wide guidelines for IT work that includes security and the system development life cycle (ITSDLC) are also within the OCIO's span of responsibility. The DOC OCIO is responsible for the action plans identified in the Federal CIO's 25 Point Implementation Plan to Reform Federal Information Technology Management include the consolidation of commodity IT spending for strategic sourcing and migration of IT services into the Cloud. This task order will support and implement these initiatives. The HCHBNet infrastructure is the primary focus of this task order. HCHBNet and DOC operating units' interconnected local and wide area networks have a key role in Commerce Enterprise Architecture, IT security, and the department's communications and operations. Other DOC bureaus located at the Herbert C. Hoover Building will leverage this task order for strategic sourcing of network and security operational services.

HCHBNet is a strategically planned, inter-networked, centralized communications infrastructure that provides connectivity for DOC automated information systems operated within the HCHB. It provides the platform for Operating Units to connect their automated information systems to one centralized core backbone in the HCHB. This backbone is logically redundant and fault tolerant and includes multiple layers of security from the external perimeter through to the data or object level of the applications and data resources accessed through the HCHB network infrastructure.

DOC designed HCHBNet as a homogeneous network that allows Operating Units (OUs) located at HCHB to transfer data, voice and video securely, reliably and efficiently. It also provides for consolidation of Operating Unit networks onto a common, standardized, high-speed infrastructure, controlled, maintained and enhanced by a central OCIO entity. DOC designed HCHBNet to evolve and scale to support new technologies and bandwidth requirements, and incorporate emerging products that permit voice, data and video to share a common, structured infrastructure that is fully documented. Technologies such as cloud services, mobility and virtualization have been incorporated into the HCHBNet.

C.1.3 AGENCY MISSION

The Commerce Department has a wide range of responsibilities in the areas of trade, economic development, technology, entrepreneurship and business development, environmental stewardship, and statistical research and analysis. Within the federal government, the Commerce Department is also the principal defender and champion of the digital economy. Data from the Commerce Department touches every American and informs daily business decisions. Commerce data enable start-ups, move markets, protect life and property, and power both small and multi-billion dollar companies. They also have a unique role in carrying out the constitutionally mandated decennial census, which serves as the basis of ensuring America's representative democracy. It determines the allocation of billions in federal dollars to states and the drawing of congressional districts, among other important activities. Within the Commerce Office of the Secretary, the OCIO provides information technology (IT) leadership advancing the mission of the Department of Commerce. It leads the management of information resources, ensuring that Commerce programs and Bureaus provide world-class information services to end users, improving the efficiency of delivering information services, and empowering and equipping a workforce that is highly motivated and customer service oriented. One of OCIO's priorities is to continuously improve secure access to data, information, and systems and to continuously protect those assets from loss or unauthorized access.

C.2 CURRENT ENVIRONMENT

The Contractor shall conform to the DOC network architecture, security, and operating procedure standards and subsequent DOC or other Government regulations, legislative requirements, industry best practices and revisions to these standards. These include:

- Format, function, data, and interface standards of HCHBNet and supporting server infrastructure.
- HCHB System Security Plan. This includes Acquisition Policy as identified in the DOC IT Security Program Policy (ITSPP). The ITSPP provides policy for the DOC and is used as the guiding policy for the HCHBNet which is managed by Office of the Secretary of Commerce (OSEC)/OCIO.
- SOPs - OITS Standard Operating Procedures. SOPs are subject to updates, additions, and deletions over time, and maintenance of these SOPs is the Contractor's responsibility.
- Commerce Enterprise Architecture: Maturity Model; Communications Plan; Configuration Management Plan; and System Development Life Cycle (ITSDLC)
- Commerce IT Security and Privacy: IT Security Program Policy; IT Privacy Policy; Electronic Transmission of Personally Identifiable Information (PII)
- Department of Commerce Scalable Project Management Methodology
- Commerce IT Investment Performance Management Policy

The current network was originally designed in 2005, but has undergone numerous upgrades, particularly within in the past 5 years. A recent replacement of access layer switches servicing approximately 5000 users throughout the HCHB was phase 1 of a 2 phase project to perform an overhaul of the existing HCHB network. The current focus is on phase 2 which consists of upgrading the core network devices that are approaching End-of-Life/End-of-Support. The replacement of core backbone infrastructure devices is needed to improve network performance and reliability of the network to meet the growing demands of high-end user computing through cloud services. The network backbone today provides a network transport for services such as wireless and VoIP to all users residing in the building. The Department has already made significant investments in these areas. Additionally, services dependent on the network backbone include video teleconferencing, cloud applications, and online collaboration. The network is physically and logically redundant and fault-tolerant comprising of access switches connected to dual distribution switches, which then connect to dual core switches. These core switches connect to dual perimeter firewalls, which currently serve as primary (active) and secondary (standby) functions. The firewalls connect to the Internet layer devices, which include multiple layers of security from the external perimeter to the data or object level of the applications and data resources accessed through the HCHB network infrastructure. The HCHBNet network topology and connectivity are comprised of a multi-layered model with three distinct layers: the Core Layer, the Distribution Layer, and the Access Layer. Additionally, a new enterprise wireless solution with network access control has been implemented in the newly renovated areas of the building.

Core Layer

The Core Layer consists of two Cisco intelligent switches. The function of the Core Layer is to move packets as rapidly as possible to one of the five Distribution Blocks. The Core has dual load sharing power supplies and redundant Supervisor Modules for resiliency.

Distribution Layer

The Distribution Layer consists of pairs of Cisco intelligent switches. The combination of a distribution switches pair and the switches connected to them are referred to as the "Distribution Block," and are used as the building block for the HCHBNet design, providing modularity and scalability. The HCHBNet defines six Distribution Blocks, which are described below. The Distribution Layer switches aggregate the traffic from the Access Layer switches. Each Distribution Layer switch includes Intrusion Detection Systems (IDS), Access Control Lists (ACLs) appropriate to the traffic for the distribution block, and redundant power supplies.

Access Layer

The Access Layer is used to concentrate endpoint devices such as workstations, phones, and printers. The Access Layer devices are currently comprised of Cisco Catalyst switches installed in telecommunications closets (Telco closets) throughout the building. Each Access Layer Switch is provisioned with two or three, and in few switches have four, 48-port 10/100 Fast Ethernet switching modules. Each switch features load-sharing power supplies and dual 1000BaseSX uplinks to the Distribution Layer switches.

The Access Layer switches connect to the Distribution Layer switches via standard IEEE 802.1q Gigabit Ethernet Trunks. The Distribution switches are connected to the Core Layer via Gigabit Ethernet fiber links (1000BaseSX). The distribution switch pair is connected to each other via an 802.1q trunk as well.

At the Distribution Layer switches, a Cisco Intrusion Detection System (IDS) Module is implemented to detect unauthorized activities (with the exception of the Management Distribution Block). The switches also apply appropriate ACLs and activity logging to restrict access to required traffic only. The HCHBNet uses a strict VLAN implementation, to isolate specific bureaus and/or other data types (i.e., VoIP is routed via a specific VoIP-VLAN).

Enterprise Wireless Local Area Network

The wireless enterprise is an integration of Cisco wireless communication devices providing client mobility throughout HCHB Campus. The wireless enterprise design consists of employing Cisco access points (APs) partially throughout HCHB Campus accompanied by two High-Availability pair Wireless LAN Controllers (WLC); one foreign controller supporting the AP population and one anchor controller supporting guest users. There is a Network Control System (NCS)/Prime Infrastructure Management server (Prime), two High-Availability pairs of Mobility Service Engines (MSE), and two Identity Services Engines (ISE) distributed between the primary and secondary datacenters for improved reliability. The WLAN and ISE authentication mechanism policy supports wired and wireless networks for peripheral systems and transport communications. The controllers and access points provide basic layer 2 and 3 connectivity to HCHBNet backbone devices upon successful authentication. For enhanced security, various client SSIDs have been implemented for guest vs. HCHB employees. The internal WLANs are non-broadcast SSIDs thus enhancing the security posture of their networks. The DOC Guest WLANs are openly broadcast reflecting the requirement for those networks to be easily accessible. Currently, there are 557 access points installed in the HCHB campus, providing wireless coverage for approximately one third of the campus. Depending on availability of budget, the intent is to have wireless coverage throughout the campus.

Network Backbone Upgrade

The existing network backbone is currently being upgraded from 1Gbps at the access, distribution and core layers. As part of the network refresh, primary and secondary uplinks between the core and distribution switches shall be converted to 10Gbps.

Existing equipment is installed in various telecommunications closets (Telco closets) throughout the campus as well as the primary and secondary data centers also located in the building.

IT Service Desk Support

The OCIO office contracts out for IT support and administration of a fully functional service desk support service for Tier 0, Tier 1, and Tier 2 services. OCIO's management and technical personnel, made up of both federal employees and contractor personnel, form the Office of IT Services (OITS). IT Service Desk (ITSD) provides support to hardware, software, and systems used to collect, process, store, transmit and disseminate data and information. This includes personal computers (desktops and laptops); hand-held computing devices; phones; tablets; printers; scanners; multi-function devices; VoIP phone system; and other peripheral IT equipment. Requirements may also involve the planning and delivery of customer support services, including but not limited to information gathering, installation and configuration of hardware and software, and assistance in response to customer service requests and troubleshooting. Tier 3 services are provided by the Systems Administration, Network Operations Center (NOC) and Security Operations Center (SOC).

OITS provides Information Technology (IT) support to the Office of the Secretary, EDA, ESA and MBDA users, which are primarily located in the HCHB. Outside the HCHB, EDA has six remote offices with approximately 120 employees that are supported through the HCHB service desk.

C.3 SCOPE

The scope of this Task Order includes the following:

- The Contractor shall provide IT service desk support services for the DOC/Office of the Secretary and three other OUs, including Economic Development Administration (EDA), Economic and Statistics Administration (ESA) and Minority Business Development Administration (MBDA).

SECTION C – DESCRIPTION/SPECIFICATIONS/STATEMENT OF WORK

- The Contractor shall provide front-line daily operations support and customer service responsibilities for the Office of IT Services. This entails basic ticket response and ensuring proper customer communications requirements are met. As appropriate, the Contractor shall be responsible for monitoring and maintaining existing security toolsets and policies to mitigate security exploits and vulnerabilities. In addition, the Contractor shall keep up with emerging security threats and information to support OCIO in meeting its mission.
- The Contractor shall respond to inquiries and resolve trouble tickets related to services managed for HCHBNet and its interconnections.
- The Contractor shall operate, maintain, and enhance HCHBNet, its interconnections, and their communications traffic. In addition to data, HCHBNet carries VOIP and legacy telephony, public address, emergency broadcast and video communications traffic.
- The Contractor shall implement IT projects that support HCHB Building Renovation, DOC Operating Units, and System Engineering and Enhancement.
- The principal place of performance will be at HCHB. Work at remote sites interconnected with the HCHB and HCHBNet are also within the scope of this task order.
- The Contractor shall provide vulnerability scanning and assessment support for systems supported by the DOC/OCIO.
- The Contractor shall maintain, operate, and engineer security enforcement tools for the HCHB network infrastructure.
- The Contractor shall provide daily monitoring, analysis, and reporting of security events and incidents as required by the DOC Incident Reporting process and procedures.
- The Contractor shall provide systems administration, Personal Identify Verification (PIV) logical access control (LAC), and server virtualization support.
- The Contractor shall provide full end-to-end support to produce, broadcast and archive events for on-demand viewing. To deliver this capability, the contractor shall provide the following services:
    - Full production support of events to include equipment, staff to set-up and break-down equipment and production services
    - On-line registration for event viewing/participation
    - Web-based transmission of recorded and live events
    - Archiving of events for streaming on-demand
    - Detailed analytical and statistical reporting on participation and viewing of broadcasted events.
- The Contractor shall operate, maintain, install, service and repair complex electronic A/V and IT systems and equipment including 70-volt sound systems, low voltage displays, and technical AV test instruments as a part of his/her normal commitment to DOC.

SECTION C – DESCRIPTION/SPECIFICATIONS/STATEMENT OF WORK

C.4 TASKS

The following tasks are in support of this TO and are detailed below:

Task 1 –Transition In/Out
Task 2 – Program Management
Task 3 - Network Operations Support
Task 4 – Security Operations Support
Task 5 – Systems Administration Support
Task 6 – IT Service Desk Support
Task 7 – Server Virtualization Support
Task 8 – HSPD-12 Personal Identification and Verification (PIV) Support
Task 9 – Building Renovation Support **(Optional)**
Task 10 – Cloud Migration Support **(Optional)**
Task 11 – New Technical Architecture and Technologies Implementation **(Optional for Option Periods)**
Task 12 – Audio Visual and VTC O&M Support
Task 13 – Live Webcast Streaming Support **(Optional)**

The skill mix and the number of labor hours in the table below are provided for estimation purposes only and may be used to provide a better understanding of the current approach to the requirements. Offerors may provide alternative solutions and/or provide alternative labor categories and hours to meet the conditions of the task requirements and deliverables.

Tasks	**Suggested Contractor Staffing**
Task 1: Transition In/Out	
Task 2: Program Management	1 Full-time (40 hours per week)
Task 3: Network Operations Support	3 Network Engineers (2 Senior and 1 Mid Level) 2 Network Security Engineer (2 Senior Level) 2 VoIP Engineer (1 Senior and 1 Mid Level) 1 VoIP Technician (Mid Level) 3 Cable Technician (2 Senior and 1 Mid) NOTE: All staff full-time (40 hours per week)
Task 4: Security Operations Support	1 Security Engineer (Senior Level) 2 Security Analyst (Mid Level) NOTE: All staff full-time (40 hours per week)
Task 5: Systems Administration Support	1 Systems Engineer (Senior Level) 2 Systems Administrators (Mid-Level) NOTE: All staff full-time (40 hours per week)
Task 6: IT Service Desk Support	1 Technical Program Manager 5 Tier 1 Support (1 Senior, 4 Mid Level) 5 Tier 2 Support (2 Senior, 3 Mid Level) NOTE: All staff full-time (40 hours per week)
Task 7: Server Virtualization Support	1 Systems Engineer (1 Senior Level) NOTE: All staff full-time (40 hours per week)
Task 8: HSPD-12 Personal Identification and Verification (PIV) Support	1 Systems Engineer (Senior Level) NOTE: All staff full-time (40 hours per week)

Task 12: Audio Visual and VTC O&M Support	1 Audio Visual/VTC Specialist NOTE: All staff full-time (40 hours per week)

C.4.1 TASK 1 TRANSITION

C.4.1.1 TRANSITION-IN

The contractor shall provide transition-in services. The contractor shall complete Transition-In services within thirty (30) calendar days of the task order start date. The contractor shall work professionally with the outgoing contractor to achieve a successful and timely transition. The contractor shall transition all services without interruption or degradation of service levels. The contractor shall verify system and facility access with the Government. The Contractor shall submit a draft transition-in plan at the kickoff meeting. The transition-in plan shall describe the approach to transition tasks and materials from the outgoing Contractor. The offeror's approach shall incorporate the following: The offeror's transition approach, process, and timelines; The offeror's approach to risk management and mitigation and ensuring disruptions are minimized; The offeror's knowledge transfer and training methodology; How the offeror will handle personnel security adjudication; and the offeror's approach to coordination with the outgoing contractor. Additionally, the transition plan shall include an extensive list of questions and issues the Contractor proposes to address with the outgoing Contractor. The contractor shall submit a Final Transition-In Plan in accordance with the deliverable table in Section F. The final transition-in plan must be detailed and include start-up activities that may be required to transition to full operational capability to successfully assume all duties under this task order. The final transition-in plan must include identification of key transition events and objectives with a corresponding completion timeline. During transition in, the contractor shall become familiar with performance requirements and establish the management organization.

C.4.1.2 TRANSITION-OUT

The contractor shall maintain complete documentation that is 100% assessable to the designated Government representatives via a web portal or some other method directed by the Government. The contractor shall overlap with the incoming contractor during the transition out period, work with Government personnel and the incoming contractor to transfer all knowledge, information and documentation for all projects and tasks related to this task order. At all times during the transition-out period, the contractor must exhibit professional conduct and work hand-in-hand with the incoming contractor to provide for a successful transition-out. The contractor shall submit a Draft Transition-Out Plan and a Final Transition-Out Plan in accordance with the deliverable table. The Final Transition-Out Plan must include all pertinent information for a successful transition, to include at a minimum:

a. Project management processes
b. Points of contact
c. Location of technical and project management documentation
d. Status of ongoing technical initiatives
e. Appropriate contractor to contractor coordination to ensure a seamless transition
f. Schedules and milestones
g. Document operational baseline

h. Actions required of the Government.
i. Effective communication with the incoming contractor
j. A final invoice and close-out schedule with the dates and actions to be completed for TO close-out

C.4.2 TASK 2 – PROGRAM MANAGEMENT SUPPORT

The Contractor shall provide program management support under this task order. This includes the management and oversight of all activities performed by contractor personnel, including subcontractors, to satisfy the requirements identified in this task order. The Contractor shall identify a Project Management Professional Certified (PMP) Project Manager (PM) by name, who shall provide management, direction, administration, quality assurance, and leadership of the execution of this task order. This position is considered a key personnel position.

- Update and manage project deliverables, risks registry, tasks and work packages, and contractor resources.
- Conduct recurring (weekly or bi weekly) and ad hoc status meeting with DOC shared services and program management team(s). Contractor shall generate and distribute meeting minutes.
- Monitor and track contractor labors hours, materials, and resources.
- Coordinate all aspects of planning and deployment with DOC, IT support contractors, and other government personnel and key stakeholders.

C.4.2.1 SUBTASK 1 - COORDINATE A PROJECT KICKOFF MEETING

The Contractor shall schedule and coordinate a Project Kick-Off Meeting at the location approved by the Government. The meeting will provide an introduction between the Contractor personnel and Government personnel who will be involved with the Task Order. The meeting will provide the opportunity to discuss technical, management, and security issues. At a minimum, the attendees shall include vital contractor personnel, representatives from OCIO and the operating units, other relevant Government personnel, the Contracting Officer and the Contracting Officer's Representative (COR).

The Contractor shall provide the following at the kickoff meeting:

- Transition-In Plan Draft

C.4.2.2 SUBTASK 2 - PREPARE MONTHLY STATUS REPORTS (MSRS)

The Contractor shall develop and provide a Monthly Status Report (MSR) using MS Office Suite applications, by the 10th calendar day of each month for the previous month. The Contractor shall submit MSRs by electronic mail to the COR. The MSR shall include the following:

- Activities during reporting period, by task (Include: On-going activities, new activities, activities completed; progress to date on all above mentioned activities). Start each section with a brief description of the task.
- Problems and corrective actions taken. Also include issues or concerns and proposed resolutions to address them.

- Personnel gains, losses and status
- Government actions required
- Schedule (Shows major tasks, milestones, and deliverables; planned and actual start and completion dates for each).
- Summary of trips taken, etc

C4.2.3 SUBTASK 3 - CONVENE TECHNICAL STATUS MEETINGS

The Contractor's Project Manager shall convene weekly and monthly with the GTR and other vital government stakeholders who will be indentified after award. The purpose of these meetings is to ensure all stakeholders are informed of project activity and (for the monthly meeting) the status report, provide opportunities to identify other activities and establish priorities, and coordinate resolution of identified problems or opportunities. The Contractor's Project Manager shall provide minutes of the monthly meetings, including attendance, issues discussed, decisions made, and action items assigned, to the GTR within five calendar days following the meeting. Conference calls, are acceptable.

C.4.2.4 SUBTASK 4 - PREPARE A PROJECT MANAGEMENT PLAN (PMP)

The Contractor shall document all support requirements in a PMP. The PMP shall:

- Describe the proposed management approach
- Contain detailed Standard Operating Procedures (SOPs) for all tasks, including updates to existing SOPs. Note: SOPs are standalone attachments to the PMP.
- Include milestones, tasks, and subtasks required in this Task Order
- Provide for an overall Work Breakdown Structure (WBS) and associated responsibilities and partnerships between Government organizations
- Provide and maintain a master schedule for all projects under this task order

The Contractor shall provide the Government with a draft PMP. The Government will comment on the draft PMP. The final PMP shall incorporate Government comments.

C.4.2.5 SUBTASK 5 - UPDATE THE PROJECT MANAGEMENT PLAN (PMP)

The PMP is an evolutionary document that shall be updated at least annually. The Contractor shall work from the latest Government approved version of the PMP to provide updates.

C.4.2.6 SUBTASK 6 - QUALITY CONTROL PLAN (QCP)

The contractor shall provide a draft Quality Control Plan (QCP) as required in Section F. The final QCP shall incorporate the Government's comments. The contractor shall periodically update the QCP, as changes in program processes occur. At minimum, the QCP shall be reviewed and updated once a year.

Within the QCP, the contractor shall identify its approach for providing quality control in meeting the requirements of the TO. The offeror's QCP shall describe its quality control methodology for accomplishing TO performance expectations and objectives. The contractor shall fully discuss its validated processes and procedures that provide high quality performance for each Task Area. The QCP shall describe how the processes integrate with the Government's requirements and not just state that they are certified in a particular quality standard approach.

C.4.3 TASK 3 – NETWORK OPERATIONS SUPPORT

The Contractor shall provide experienced and qualified professional personnel to provide services to include, but not limited to the following:

- Operate and maintain the network hardware, applications and tools that support the Network Operations Center services. This includes telephone services, HCHB network infrastructure operations support and network security management services. This applies to the Operating Units and commercial entities in the HCHB as well as any of their remote sites that have migrated to the HCHB network infrastructure. Service desk tickets referred to the network operations center (NOC), for telephones, or for the public address system and emergency broadcast system (EBS) are also included.
- Replace hardware and software to support the performance measures listed in the service Level agreements (SLAs) (see Section J). The OCIO, based on a business case, must approve any introduction of new hardware or software brands not currently in the HCHB network infrastructure's inventory. Provide an equipment and maintenance refresh schedule. Maintain an inventory of all hardware and software that supports the HCHBNet. Re-architect and implement migration; make appropriate changes to network zones and enclaves. The hardware refresh cycle is currently 3-5 years for servers and 5-7 years for network equipment; hardware and software costs are reimbursable under the ODC CLIN.
- Move, add, and change network hardware and/or software when it is not associated with building renovation. The Contractor shall remove, replace, upgrade, and/or install cable plant, racks, panels, and other infrastructure that is not associated with building renovation. Cable plant and cable moves, adds, and changes associated with office renovation (CD410's) but not HCHB building renovation are within the scope of Task 3. The contractor shall purchase miscellaneous consumables to supply these moves, adds and changes through the ODC CLIN.
- Provide NOC and SOC operations during core business hours, which are 7:00 a.m. – 6:00 p.m. Monday through Friday (except Federal holidays); special weekend/nighttime requirements (e.g., maintenance and upgrades); and emergency after-hours on-call staff support (including contact information) for assistance at all other times. The Contractor shall obtain approval from the GTR and COR for work outside core business hours.
- Conduct real time network monitoring of HCHBNet performance and usage; and provide weekly, monthly and quarterly reports to management on the health, stability, utilization and any changes made to the HCHB network infrastructure.
- Document new and update Standard Operating Procedures (SOPs) as a result of new tools, systems and/or processes.
- Provide integrated, transparent network maintenance, including the cable plant. Document the required maintenance and obtain approval via the Change Control Board process (Section J) prior to conducting the network maintenance.

- Receive audible Public Address System emergency broadcast successfully during normal working hours in all HCHB common areas.
- Provide support for existing wireless infrastructure that is connected to the HCHB network infrastructure. Approximately 560 Cisco wireless access points have been deployed in the HCHB campus. Both guest wireless and internal wireless networks need to be managed.
- Log and track all telecommunications and network-related customer service requests from receipt of request to completion of service via the Service Now tracking system in real time. ServiceNow is purchased as a service for the government and operated by the contractor. Monitor email notification of Service Now tickets assigned to the NOC. Respond to Service Now tickets. Update ticket with diagnostic, corrective, referral or other dispositive actions taken. Route to other responding activities when appropriate. Close out assigned trouble tickets when completed.
- Trouble ticket receipt may be by referral from the OCIO IT Service Desk, direct to Contractor's staff, or from other sources. Request may be received from other customers within HCHB as other service desks exist within HCHB. The awarded contractor will maintain the OCIO ITSD.
- Respond to and resolve tickets within SLA standards (see Section J) via Service Now (Fuiji user interface) through the OS/OCIO IT Service Desk.
- Maintain current, detailed HCHB network infrastructure diagrams and drawings.
- Establish maintenance agreements with the equipment manufacturer(s) for the backbone equipment that will allow advance replacements (expedited delivery of emergency replacements) for failed units/modules. These maintenance agreements shall cover Internetworking Operating System upgrades to ensure bug fixes and software releases are provided. The Government will procure CISCO smartnet through a separate contract vehicle. All other maintenance agreements will be reimbursable under the ODC CLIN.
- Provide customer service that can be monitored by relevant metrics to include, but not limited to reports on timeliness of response to service requests, effectiveness of communications, compliance with formal service desk ticket processing procedures, and the results of customer surveys.
- The Contractor shall also support moves, adds and changes for analog, IITSDN, T1, T3, special circuits, ATM from the local carrier for faxes, modems, elevator, and STE. Maintenance of HCHBNet wiring inside HCHB is also the Contractor's responsibility. If there is a failure of dial-tone from the local carrier, the NOC Contractor will coordinate with the Government prior to any maintenance. The NOC Contractor may also, with coordination with the Government, request a new line, new number or other service from the local carrier performed via an online portal. However, the analog phone service contract is between the Government and the local carrier, not with the NOC Contractor.
- Safeguard Government-provided property, including keys, sensitive data, personal computers, miscellaneous office equipment and furniture, and office/storage space, etc. Secure space for storage will be provided.
- Perform remedial maintenance after hours, during periods when it does not disrupt or impede the DOC customers.

- Provide administrative, analytical and implementation support to DOC customers for services offered under the WITS 2003, Networx and the GSA follow-on contract to WITS3 and Networx task orders. Provide consulting support to assist with the technical aspects of the disconnection and transition from WITS 2003 and Networx to the GSA follow-on contracts.
- Perform preventative network maintenance and upgrades on network hardware and tools to ensure that network is operating at optimal performance.
- Implement security patches and bug fixes to mitigate security vulnerabilities and known defects in accordance with best practices and to be in complaint with DOC security policies (see Section J).
- Provide artifacts to support Accreditation and Authorization activities.
- Review network aspects of building renovation design. Review GSA construction concepts, designs and other material and drawings as they relate to network and telecommunication renovation activities. Provide comments and recommendations with respect to network aspects of building renovation, i.e., cable plant, network servers, internetwork operating system, other network subsystems, racks, cable paths, power, cooling, monitoring, and security.
- Develop weekly activities reports and other reports in accordance with the task order deliverables requirement

C.4.3.1 SUBTASK 1 - DATA CENTER SUPPORT

- Monitor all software and hardware products and ensure compliance to Data Center standards and best practices.
- Coordinate with IT Manager and other business units to develop strategies to ensure achievement of data center capacity.
- Analyze and determine appropriate layout of all equipment in data center for adequate power and cooling requirements.
- Monitor all data center activities such as new equipment installation or removal or disposal of existing equipment.
- Document all power and space schematics and ensure accuracy in same.
- Perform installation and ensure effective layout of all tools (Section J) in accordance to industrial standards and best practices.
- Monitor all data center assets for tracking and audit purposes.
- Coordinate with vendors and organization IT staff to ensure effective completion of all installation hardware.
- Perform capacity planning and power and cooling audits to ensure adequate power and cooling are supplied to service equipment.
- Maintain access control log to the data center and ensure appropriate filling of all columns in Sign-in sheet. Maintain Sign-in sheets for audit purposes.
- Monitor all issues and escalate issue as appropriate to specific IT organizations for prompt resolution.
- Ensure compliance with data center best practices and standards to ensure life safety is adequately provided and adhered to in the data center.

- Maintain standards of service levels at all times, ensure response with timeframe and manage all available services.
- Document Standard Operating Procedures and policies and best practices relating to data center operations.
- Attend HCHB Change Control Board meetings.
- Keep data center clean at all time and ensure compliance with appropriate use of data center.

C.4.3.2 SUBTASK 2 - VOIP PHONES SUPPORT

- Operate and maintain existing Voice over Internet Protocol (VoIP) Phone System and its hardware and tools.
- Provide Moves, Adds and Changes (MAC) support on the Cisco and Unity Voicemail product for over 4,000 network and phone support users in HCHB. Ensure that phones are configured, registered to the phone management system and assigned to the right individuals. As appropriate, troubleshoot and resolve problems relating to the phones or phone management system.
- Document network characteristics for baseline and stability metrics and escalate troubles/problems to the NOC engineers.
- Coordinate moves with the building management staff as well as coordinate the activities of the NOC staff.
- Coordinate with the Local Exchange Carrier, Cisco, and other vendors.
- Serve as telecommunication tier 1 support for the customer on all telecom system performance (voicemail, fax line dial tone problem, Cisco IP phone device problem, Call accounting reporting).
- Troubleshoot technical problems with customer's phone device, voicemail and fax machine lines within HCHB.
- Interface and submit requests to Verizon WITS in reference to analog lines or trouble shooting DID line problems
- Update the CDR Infortel call accounting system and inventory of the active DID's or deactivated lines
- Provide and instruct users on the functionality of the Cisco IP phone product features, as well as with the Unity Voicemail product
- Ensure customer requests are routed to the proper NOC or IT group for resolution
- The VoIP technician will document all procedures, troubleshooting steps and SOW's related to this position. The VoIP technician will also update and verify existing support documentation and will work with the NOC team and ITCSC management.
- Input user information from Cisco Call Manager in order to reflect accurate reports for the line count report that is submitted annually for budgetary and charge back to customers.
- Semiannually review the Cisco Call Manager to ensure that the manager IDs are up to date to reflect office names.

C.4.4 TASK 4 – SECURITY OPERATIONS SUPPORT

- Actively monitor the HCHB network infrastructure and network audit logs for potential breaches in security and implement appropriate remediation. Remediate security problems identified by the Security Operations Center (SOC) or another responsible source.
- Provide real time monitoring and situational awareness of security events and first tier incident response and escalation to the DOC Enterprise Security Operations Center (ESOC) per DOC incident response policy and procedures.
- At least one member of the team shall be cleared at the Top Secret level to provide support to the DOC ESOC in response to classified security incidents detected via the Einstein Intrusion Prevention Security Services (IPSS).
- Maintain and enhance existing DLP capability and services to support active blocking of Personally Identifiable Information and any other information identified in DOC policies for the HCHB campus infrastructure and supported components and develop dashboard reporting elements for Senior and executive management;
- Manage and maintain security endpoint management solution for the Office of the Secretary and supported operating units.
- Conduct regular vulnerability scanning, reporting and assessment of OCIO supported systems.
- In coordination with the GTR and Managed Trusted Internet Protocol Services (MTIPS), review and manage security policies enforced at the MTIPS inspection Level for HCHB.
- Perform annual review and updates of policies for security tools on HCHBNet
- Note: On average, 25-30 scans are run a month

C.4.4.1 SUBTASK 1 - NETWORK AND SECURITY ENHANCEMENTS

- Configure new network and security hardware and software to maximize the performance of the HCHB network infrastructure. No contractor furnished equipment is requested, equipment will be government owned/contractor operated. Develop Implementation/Upgrade Plan to include project schedule. Document new installations with screenshots to capture specific configuration and settings.
- Stay abreast of technology and recommend technology refreshment and/or new technology, including IT security awareness.
- Provide NOC on-site Continuity of Operations (COOP) support for relocated Office of the Secretary (OSEC) personnel at designated COOP locations. Note: the NOC does not provide a true COOP site; Operating Units and staff offices provide their own COOP plans and facilities. This is only relevant in a real world COOP event. NOC staff is not required to support annual COOP exercises.
- Provide Homeland Security Presidential Directive-12 (HSPD-12) implementation support. Make firewall rule and network changes so that Personal Identify Verification (PIV) cards can be used to authenticate users to the HCHB network infrastructure. The objective is to authenticate users to the Active Directory domain using PIV cards. The

NOC Contractor shall only be responsible for the network tie-in and not the actual HSPD-12 or PIV cards implementation.

- Maintain and operate a Dual Stack IPv4 and IPv6 environment. Complete migration of HCHBNet to IPV6 from IPV4. This includes planning, testing and implementing IPV6 to the HCHB network infrastructure. The Contractor shall implement all routing and firewall rules to support IPV6.
- Maintain and operate Passive Optical Network (PON) that will be deployed as the HCHB building is being renovated. Anticipated PON deployment will be in the Renovation Phase 4 project scheduled to be operational sometime in March/April of 2018.
- Upgrade, replace and enhance existing HCHB-wide network infrastructure security equipment including the Intrusion Detection and Prevention Systems as part of Security Operations which will be provided as government furnished equipment.

C.4.4.2 SUBTASK 2 -TESTING

- Provide routine maintenance, failover testing, and adjust or correct the HCHB network infrastructure outside normal working hours (after 9:00 p.m. during the week or on weekends as outlined in the Change Management Policy and Procedures and Standard Operating Procedures).
- Conduct complete testing of network software and hardware in the DOC lab and provide documented results to the Change Control Board for approval prior to implementing any change to the HCHBNet production environment.
- Test the Emergency Broadcast System (EBS) once each weekend, as a minimum, for technical correctness; and during core business hours once monthly, as a minimum, for functional correctness.
- Test the Public Address System after hours at least monthly to ensure technical correctness. The Contractor shall provide any required maintenance after regular business hours.

C.4.4.3 SUBTASK 3 - PROCESS AND REPORTING

- Provide reports to the GTR and OCIO management that include:
  - Weekly, monthly, quarterly statistical reports that address the network performance goals and objectives in the SLAs (see Section J). All network support activities (e.g., trouble calls, service requests, special projects, scheduled maintenance, etc.), as well as reports concerning infrastructure system health, executive summary reports requested by the Government Task Manager and utilizing ServiceNow database and other sources; and,
  - Weekly, monthly, quarterly statistical data that address the HCHB network, VoIP and Emergency Broadcast system performance goals and objectives in the SLAs. The data shall include bandwidth utilization data, any service outages, historical service desk data (types of services provided, to whom, response times, Quality of service for the network/voice operations, PRI utilization, Security Audit Reports, etc.) and management reports.

- Develop, maintain and enforce Standard Operating Procedures (SOPs) for the NOC and SOC services rendered. Update the SOPs with the changes as appropriate. Comply with current and new SOPs.
- Conduct management briefings once a week.
- Maintain baseline of network utilization and performance metrics to include applications and traffic patterns.
- Continuously review the NOC and SOC operations and devise/report on ways to improve delivery of services and customer satisfaction.
- Provide monthly reports on Operating Units' telephone lines count.
- Provide quarterly HCHBNet node count reports.
- Comply with DOC Change Management Policy and Procedures and IT Security Policy (see Section J) provided in separate attachments.
- Maintain and update all NOC and SOC equipment inventory semiannually. All reporting is performed through GFE equipment. Follow SOPs for handling of equipment and inform DOC customer of equipment relocation/decommission. Assist OS property custodian with tracking of equipment per the DOC Property Inventory Audit.
- Maintain annual asbestos training for NOC Cable Infrastructure 5. Training will be provided by building management.
- Provide support and data on network and security configurations to the IT Security officer to remain in compliance with FISMA requirements with artifacts. This includes annual security Assessment and Authorization (A&A) activities and quarterly FISMA reports to the Office of Management and Budget (OMB).
- Maintain security patches on all NOC and SOC systems in accordance with DOC Security Policy (CITR-016 and CITR-017) (Section J).

C.4.5 TASK 5 – SYSTEMS ADMINISTRATION SUPPORT

C.4.5.1 SUBTASK 1 - TIER 3 SYSTEMS ADMINISTRATION SUPPORT

Operate and manage the hardware, software and tools that support the Windows Active Directory environment.

Deploy, manage and maintain Windows servers.

Manage and maintain GPOs, Active Directory, DNS, File/Print server.

Participates in technical research and development to enable continuing innovation within the infrastructure.

Ensures system hardware, operating systems, software systems, and related procedures adhere to DOC standards.

Install new/rebuild existing servers and configure hardware, peripherals, services, settings, directories, storage, etc. in accordance with standards and projects/operational requirements. All equipment is GFE.

Develop and maintain installation and configuration procedures.

Contribute to and maintain system standards.

Research and recommend innovative, and where possible automated approaches for system administration tasks. Identify approaches that leverage resources and provide economies of scale.

Perform daily system monitoring, verifying the integrity and availability of hardware, server resources, systems and key processes, reviewing system and application logs, and verifying completion of scheduled jobs such as backups.

Perform regular security monitoring of systems to identify any possible intrusions.

Provide Tier III support. Investigate and troubleshoot issues.

Document SOPs on supporting the Active Directory environment.\

Apply OS patches and upgrades to administrative tools and system in accordance to CITR-016 or DOC and/or federally mandated requirements to address high to critical level vulnerabilities. BigFix and LanDesk are the current patching platforms. Maintain operational and configuration procedures.

Perform periodic performance reporting to support capacity planning.

Perform ongoing performance tuning, hardware upgrades, and resource optimization.

Provide architecture and engineering support for customer applications, system interoperability and security.

Provide support for DOC Office of Security (OSY) managed systems, including user access and backup considerations. Provide support to install, configure, upgrade, monitor, optimize and maintain application databases and regular patches.

C.4.5.2 SUBTASK 2 - TIER 2 SYSTEMS ADMINISTRATION SUPPORT

- Provide support for account creation and deletion for approximate base of 1500 full service desk support users; average yearly creations: 632, deletions: 487 and modifications: 255.
- Analyze applications and network systems to plan, design, evaluate, and select operating systems and Desktop compatible components/peripherals. Responsible for assisting the Senior LAN Administrators with capacity planning, configuration assessment of workstations, laptops, mobile computing, NAS/SAN storage and other communications and peripheral devices.
- Provide support for new technologies to ensure interoperability with the LAN.
- Provide weekly statistics to upper management
- Develop and implement Standard Operating Procedures (SOPs) for the New Technologies.
- Establish secure computing environment by designing system configuration; directing system installation; defining, documenting, and enforcing system standards as they relate to the customer's desktop and mobile computing environment. This includes conducting site surveys, project meetings, installation and post-installation issues.
- Provide support of LAN equipment during outages, maintenance windows and equipment relocation. This task is usually performed after hours.

- Maximize effectiveness of the LAN environment by monitoring performance; troubleshooting operational problems and outages; scheduling upgrades; and developing processes on optimization.
- Provide support and account set up for the VPN access through the RSA system.
- Perform daily backup operations, ensuring all required file systems and system data are successfully backed up to the appropriate media, recovery tapes or disks are created, and media is recycled and sent offsite as necessary.
- Maintain and upgrade software elements, including the operating system
- Troubleshoot software and hardware issues
- Troubleshoot configuration problems
- Assist with maintenance of proper version of the installed software elements, including bug fixes and security
- Assist with data-spill cleanup, sanitization, and computer malware eradication in accordance with DOC and local policies and procedures with direction from DOC and security team
- Ensure that DOC is aware in writing of improperly performing equipment and assist on replacement/repair of such equipment
- Update and maintain desktop/laptop images on a regular basis or when new applications are added to the environment.

C.4.6 TASK 6 – IT SERVICE DESK SUPPORT

The contractor shall provide the expertise, technical knowledge, staff support and other related resources necessary to:

- Provide a Single Point of Contact (SPOC) for initial reporting of incidents
- Provide configuration, maintenance, and support for the existing ServiceNow (SNOW) Incident Management System (IMS) that integrates with existing DOC systems (such as LANdesk and BigFix) for incidents, requests and asset management. SNOW must be automated and aligned with Information Technology Infrastructure Library (ITIL) v3 standards. ServiceNow is government owned and contractor operated.
- Support for SNOW shall include the following nine modules:
    - Incident Management
    - Problem Management
    - Change Management
    - Knowledge Management
    - Release Management
    - Service Catalog
    - Configuration Management Database
    - Asset Management
    - Project Portfolio Management
- Process incidents/problems per defined SLAs
- Establish and maintain a Tier 0 self-service capability

- Provide Tier 1 on-site incident management support
- Provide Tier 2 on-site support for escalated tickets
- Provide management support to Tier 0, 1, and 2 operations
- Provide transition support and ensure continuity of operations
- Provide additional services, to include the following:
    - Surge projects and technology enhancements
    - Hardware and software purchases refresh activities
    - Travel to remote sites
    - Training support for ServiceNow feature enhancements which may include online or instructor-led sessions.
    - Extended hours of operation to support surge projects
    - Additional SLAs
    - Comprehensive application support
- Note: Annual total for first call resolution was 5,367 from a total of 25,819 calls for FY16.
- Note: No customer satisfaction rates have been measured to date
- Note: Mean time to respond and mean time to resolve metric for the past year are not available.

Tier 0, Tier 1, and Tier 2 activities are defined with the following tasks:

TIER	TASKS
Tier 0	• Develop documentation, establish a self-service portal and associated knowledge base, and maintain updated information for users to obtain self-service such as FAQs and web-based entry of service requests • Current self-service and knowledge base is minimal and out dated. Expectation is contractor will expand both features and keep them current. • Tier 0 self-service capability exists but is not utilized and kept current. • Password reset may also be included in the self-service system
Tier 1 (on-site)	• Serve as first point of contact for users • Log user calls, manage incoming service requests and incidents, create, update, and monitor all tickets • Track tickets until closure and update customer • Resolve all service requests that do not require escalation to higher tiers of service • Provide basic incident evaluation, fault isolation, analysis, and troubleshooting, resolving all incidents that do not require escalation to higher tiers of service • Use remote diagnosis and tools if applicable to resolve incidents • Escalate incidents to the appropriate tier based on SLA guidelines and dispatch on-site support as required
Tier 2 (on-site)	• Resolve service requests that required escalation to Tier 2 • Provide specialized/administrative on-site support: incident analysis, fault isolation, troubleshooting, and remedial/restoration actions after escalation to resolve ticket • Assist user with hardware incidents • Set up user accounts and workstations, provide scanning and virus remediation, manage loaner pool by configuration devices • Update tickets for all activities performed

	• Analyze trends and provide weekly management and user reports • Coordinate with external contractors for assets under warranty • Escalate incidents to the appropriate tier based on SLA guidelines • Image, test and deploy standard configurations for desktops and laptops. • Provide 24/7/365 support to DOC Secretary and staff.

C.4.6.1 SUBTASK 1 -TECHNICAL MANAGEMENT SUPPORT

- Provide oversight of the IT Service Desk operations by ensuring adequate resources are assigned to resolve problems and issues in accordance with established SLAs.
- Provide weekly and monthly activities report to OCIO Task Manager.
- Provide pending tickets status.
- Interface regularly with other IT groups for situational awareness with upcoming projects and planned system maintenance.
- Attend meeting with OCIO Task Manager and management when requested.

C.4.6.2 SUBTASK 2 - TIER 2 SUPPORT

- Conduct desk side visit with customers to resolve issues that cannot be addressed remotely.
- Repair and replace desktop/laptop hardware and parts where applicable.
- Install image, download drivers and application latest version and patches on desktops/laptops.
- Troubleshoot and resolve Windows Office applications.
- Perform regular file archival and purge as necessary.
- Create, change, and delete user accounts per request.
- Perform hardware maintenance on equipment that is maintained in-house
- Configure, install, and troubleshoot DOC-approved laptops, desktops, phones, tablets, network-connected multi-function devices, and other office IT equipment
- Configure, install, and troubleshoot DOC-approved software elements including the operating system (OS)
- Escalate hardware repair/replacement issues to DOC-contracted hardware vendors
- Ensure all portable IT equipment is current and ready for immediate deployment at all times
- Track status and whereabouts of all checked-out equipment and ensure checked-out equipment is returned on time. Loaner equipment should be secured and locked when not in use
- Support international travel program (includes device scanning, laptop wiping, and issuing of devices).
- Provide 24/7/365 support to DOC Secretary and staff.

C.4.6.3 SUBTASK 3 - TIER 1 SUPPORT

The Contractor shall provide impact and priority-based incident categorization in order to track progress of all incidents and restore degraded or disrupted services as quickly as possible. Contractor shall:

- Conduct initial triage and assign and escalate to other IT support organizations as appropriate.
- Provide a ITSD support structure that allows for escalation of incidents based on expertise required for resolution and urgency
- Answer customer telephone calls and emails to the ITSD in accordance with the applicable SLAs during normal working hours (NWH).
- Monitor all channels of incoming requests (emails, voicemails, submissions through the self-service portal)
- Log incidents and service requests into the IMS. Ensure that all incidents are promptly and accurately documented in IMS so that up-to-date information is available at all times. Track incidents from first report to remediation and closure.
- Perform initial diagnosis and analysis of Incidents and provide immediate resolution and recovery whenever possible. Use remote control tools to assist and resolve customer incidents as initial resolution, providing warm handoff escalation of Incidents that cannot be immediately resolved
- Escalate tickets as required
- Communicate system outages in accordance with established SOPs to appropriate DOC points of contacts and Users using DOC-provided tools and communication methods and continue ongoing communications until the Incident has been resolved and all services have been restored
- Follow-up on resolved Incidents to check quality, get customer concurrence of Incident closure, and to report customer satisfaction
- Work with Operational and other teams to ensure final summary, review, analysis, resolution, and lessons learned are documented in Incident Reports for all major Incidents and unplanned service outages, and submitted in writing to DOC management
- Establish and maintain and update information in the Known Error Database using existing material for reference; document workarounds and generate known error sub-processes to facilitate quicker diagnosis and resolution for future Incidents
- Proactively monitor Automatic Call Distribution (ACD) calls, Incidents and Service Request work flows, processes and queues to immediately identify and address performance issues that will impact the delivery of services to users
- Ensure non-IT requests are properly routed to appropriate support organizations.
- Provide live telephone coverage during NWH of service via a Contractor-owned call distribution system. All equipment will be GFE.
- Answer calls in the order they are received in accordance with applicable SLAs (see attached).
- Conduct triage support in accordance with Industry best practices.

- Continuously monitor the ITSD email queue for new requests or establish process/system to automatically route new requests to the ticketing system
- Create tickets in a manner that meets and/or exceeds applicable SLA
- Verify information with the end user, as required
- Provide user with a ticket number and record in ticket system
- Address any after-hours requests the next business day when NWH resume
- Update tickets in a manner that meets and/or exceeds applicable SLA
- Monitor critical events that come to the ITSD via any means, such as the network monitoring systems, phone call, e-mail, etc. These events could be associated with issues such as data spills or loss of data, customer unsatisfactory responses, and others determined to require immediate assistance and potential intervention.
- Make critical events available to all ITSD agents for real-time reference
- Create tickets and manage resolution process in a manner that meets and/or exceeds applicable SLA
- Update tickets by adding work log information as required by the applicable SLAs
- Monitor status of all open tickets and escalate as required
- Coordinate resolution with other internal and external teams, as appropriate
- Check the assigned tickets queue on regular basis throughout the NWH
- Provide advice and guidance to the Users regarding restoration of interrupted service
- Verify ticket resolution with the User
- Provide advice and guidance to Users regarding restoration of interrupted service.
- Require that no ticket be closed without concurrence from the User that the issue represented by the ticket has, in fact, been fully resolved and that the service has been restored. When an issue is resolved, the Contractor shall change status of the ticket to "Resolved".
- Make no more than three (3) attempts within a six-day period to contact the User to secure an agreement to close the ticket.
- Assume all responsibility for resolving Incidents in a manner that meets or exceeds the applicable SLAs. It is the responsibility of the Contractor to escalate and/or seek assistance from DOC if other support teams are not being responsive to requests for assistance. The Contractor shall maintain status of all open tickets in a manner that meets the SLAs.
- Continuously review Incident data as well as other sources of information to identify trends that may lead to discovery of a common cause of incoming Incidents. When such a cause is determined, the Contractor shall create a Problem ticket and link all related Incident tickets to it. Upon resolution of the Problem ticket, the Contractor shall update all related Incident tickets.
- Log and track requests for IT components and services, and deliver approved IT components
- Log Service Requests into the IMS. Ensure that all Service Requests are promptly and accurately documented so that up-to-date information is available at all times
- Follow-up on completed requests to check quality, get customer concurrence of request closure, and to report customer satisfaction

- Establish (or update existing ones) and maintain an equipment checkout system for short-term assignments of laptops and other portable IT equipment
- Monitor processes that coordinate delivery of IT assets directly to customers and office equipment custodians. Ensure User in/out processing is factored into the process.
- Serve as the ticket "owner" of the resolution process from the initial contact with the Users to resolution of the Incident, Problem and Service Requests. The ITSD Contractor shall assume responsibility for Incident, Problem and Service Request resolution regardless of the party actually performing the work, i.e., if the work is performed by an organization external to the ITSD, the ITSD is still responsible to track the resolution and escalations, as required by the SLAs.
- Notify Users about planned maintenance windows and outages via user Broadcast emails. The Contractor shall make use of the ACD/Interactive Voice Response (IVR) system to notify Users about unscheduled service interruptions as soon as possible after the unscheduled service interruption is confirmed.

C.4.6.4 SUBTASK 4 - TIER 0

- The Contractor shall establish and maintain a Tier 0 self-service capability for DOC users. This capability should include a knowledge base for user inquiries and help concerning commonly asked or requested services to be available on a self-service portal.
- DOC expects that a significant portion of today's typical Tier 1 tickets can be diverted to Tier 0.
- The Contractor shall utilize existing materials as well as develop new documentation to use on the portal. Information shall be updated for users to obtain self-service such as FAQs and web-based entry of requests. Some documentation and FAQs may be posted on the DOC external website to assist users who are unable to log in to the system.
- The Tier 0 system may include a capability for password resets. Applications supported by the password reset system will be determined during the transition period.

C.4.7 TASK 7 – SERVER VIRTUALIZATION SUPPORT

- Operate and manage the hardware, software and tools (see Section J) that service the Server Virtualization environment.
- Operate and manage the SAN and Backup solution servicing the Server Virtualization environment.
- Build, configure and manage virtual machines.
- Configure and test all Windows server configurations in accordance with the appropriate NIST Security Configuration Checklist.
- Develop, implement, maintain and update Standard Operating Procedures (SOPs) for the Server Virtualization and its critical components.
- Provide node management, maintenance, and troubleshooting efforts for projects critical to the business.
- Provide technical leadership and mentoring to the virtualization team.

- Perform the operations daily health check to ensure that the network storage is operational.
- Provide Tier3 support in troubleshooting of the storage & virtualization network related issues and problems.
- Lead and coordinate troubleshooting.
- Resolve and close tickets in accordance with government/ customers SLAs.
- Ensure that the storage and its components are patched with the latest software version, security updates, and hotfixes.
- Conduct research on best practices to improve performance and enable storage/ virtualization environment stability and availability.
- Cross-train and mentor other engineers to improve coverage and team performance.
- Provide On-call rotation duty.
- Conduct after hours maintenance and troubleshooting as required.

C.4.8 TASK 8 – HSPD-12 PERSONAL IDENTIFICATION VERIFICATION SUPPORT

- Provide daily administration and operations support for windows authentication to approximately 1500 users using HSPD-12 Personal Identity Verification (PIV) cards.
- Provide compliance reports (bi-weekly) for PIV authentication enforcement.
- Utilize the Government provided Quest Migration Manager tools to perform all aspects of the Active Directory testing, implementation, recovery and account verification and integrity.
- Perform work on all phases of data security, quality control, data recovery and backup during the migration process.
- Configure and test all Windows server configurations in accordance with the appropriate NIST Security Configuration Checklist.
- Test, troubleshoot and resolve issues relating to PIV authentication.
- Provide enhancement support to integrate two-factor authentication for applications using PIV cards.

C.4.9 TASK 9 – BUILDING RENOVATION SUPPORT (OPTIONAL)

- Provide HCHB network and telecommunications implementation to support Building Renovation project. DOC's renovation will affect every space within the HCHB. Construction will take place throughout the Period of Performance of this Task Order. Throughout the life of the HCHB renovation project, the Contractor shall fulfill renovation network and telecommunication requirements.

  The Building Renovation schedule is provided below:

Phase 1	*January 2008 – November 2009*	Replace air conditioning system cooling towers. Build the swing space to house staff while future phases of the building renovation are in progress.
Phase 2	*July 2009 – July 2012*	Interior and exterior renovations will encompass Corridor 1 along Constitution Avenue. This includes new mechanical, electrical, and plumbing systems, and architectural finishes (e.g., casework, molding, paneling). Phase 2 work also

		includes facade restoration and site utilities replacement around the entire building, and developing a staging area for construction materials. Staff moves out of Swing Space and Corridor 2 areas on June 15, 2012; moves will be complete by July 2012.
Phase 3	*November 2011 – August 2014* ***Pilot Project:*** *February 2014 – July 2015*	Interior and exterior flat roof renovations will encompass Corridor 2 (second corridor north of Constitution Avenue). This includes new mechanical, electrical, and plumbing systems, and architectural finishes. The DOC Federal Credit Union relocated to an area off the Reagan Building tunnel.
Phase 4	*September 2015 – May 2018*	Interior and flat roof renovations will encompass Corridor 3. This includes new mechanical, electrical, and plumbing systems, and architectural finishes. The Fitness Center relocated to the basement level, Corridor 3.
Phase 5	*April 2018 – November 2020*	Interior and flat roof renovations will encompass Corridor 4. This includes new mechanical, electrical, and plumbing systems, and architectural finishes.
Phase 6	*November 2020 – July 2022*	Interior and flat roof renovations will encompass Corridor 5. This includes new mechanical, electrical, and plumbing systems, and architectural finishes. Paper Clips will be relocated to the basement level, Corridor 5. The Child Care Center will be relocated.
Phase 7	*April 2023 – January 2025*	Interior and flat roof renovations will encompass Corridor 6. This includes new mechanical, electrical, and plumbing systems, and architectural finishes.
Phase 8	*April 2025 – January 2027*	Interior and exterior renovations will encompass Corridor 7 are. This space will be returned to GSA.
Retrofit Phase 2	*April 2025 – August 2026*	Update previously renovated space to 21st Century Workplace design.
Retrofit Phase 3	*September 2026 – November 2027*	Update previously renovated space to 21st Century Workplace design.

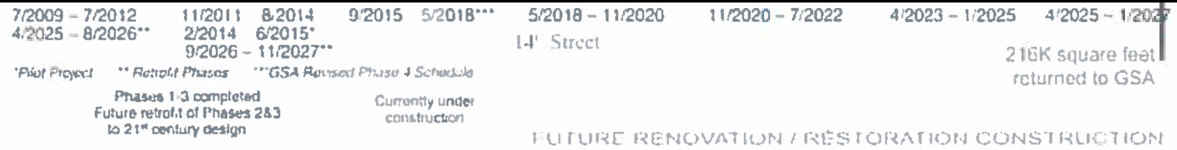
- The Contractor shall remove, replace, upgrade, and/or install cable plant, racks, panels, and other infrastructure associated with building renovation. Provide all network moves, additions and changes for all employees remaining in the HCHB, to include continuous HCHB network, telephone, emergency broadcast and desktop services during the renovation project. This includes the network cable plant up to the point of cable termination but excludes desktop devices (computers, telephone handsets, printers and other peripherals are excluded). The contractor shall provide miscellaneous materials such as cables, connectors and patch panels to support the move, add and change. These materials will be reimbursed through the ODC CLIN.
- The Contractor shall cooperate with other Government and contractor organizations participating in the renovation project, and shall ensure that network support does not adversely impact the renovation schedule.

- The Contractor shall perform network move, add and changes for areas that have been renovated. These renovated areas are issued Work Authorization form CD410t that identifies the required system furniture and supporting network cables layout. Work that exceeds the threshold (10 new cables run per request) will be supported via this task. Cables installation of less than 10 new cables fall within the NOC Operational and Maintenance Support under Task 3.
- Contractor shall provide support with the planning and execution required to successfully relocate network equipment to prevent damages to these devices. Contractor shall perform these tasks during approved maintenance window to ensure minimal disruption to NOC services.
- Contractors shall provide support with the planning and execution to successfully relocate networking equipment and services from A001 to the new NOC Secondary Core Room in the Phase 5 (Corridor 4) areas. Contractor shall establish network connectivity from the new NOC Secondary Core Room to existing Telecommunications closets.
- Conduct Quality Assurance for all fibers and copper cables installed in the renovated areas. The Contractor shall test and validate that the fibers and cables are properly implemented in accordance with standards and procedures and in compliance with other governing regulations and policies.
- Survey the areas to be renovated and if required, establish network connectivity for users impacted by the decommissioning of the telecommunication closets located in those areas.

HCHB Renovation Phases

(b) (5), (b) (7)(F)

[redacted]



C.4.10 TASK 10 - CLOUD MIGRATION SUPPORT (OPTIONAL)

The Contractor shall provide engineering and new technologies implementation. The Contractor shall provide hardware, software, and process innovations that depart from the existing technical architecture and so are within the scope of Task 10.

- Provide technical support for migration of DOC/OCIO applications, data, and other resources to the cloud. This includes research and development, design and migration support to ensure successful migration to the cloud.
- Develop an engineering and design plan to migrate the virtualized server environment to the cloud. Assist with the migration effort to minimize services disruption.
- Note: Excluded are the cloud platforms, which DOC/OCIO will procure from another source or which the Contractor will purchase under the ODC Ancillary Products/Service CLIN.
- Note: Innovation environments within vendor's labs is permitted if on the vendor's time, equipment and funded by the vendor.
- Note: Both on premise and public cloud solutions will be considered

C.4.11TASK 11 – NEW TECHNICAL ARCHITECTURE AND TECHNOLOGIES IMPLEMENTATION (OPTIONAL FOR OPTION PERIODS)

The Contractor shall provide engineering and new technologies implementation. The Contractor shall provide hardware, software, and process innovations that depart from the existing technical architecture and so are within the scope of Task 11.

- Identify, analyze, develop, plan and propose for deployment new or emerging technical architectures that depart from the current DOC/OCIO technical architecture. Document this analysis and plans for DOC/OCIO management consideration.
- Implement new technical architecture consistent with DOC/OCIO guidance. Examples: central server to client server; centralized to distributed; proprietary to open systems; web enabling systems and applications; Windows to Linux; independent to consolidated networks; other topological changes.
- Develop an engineering and design plan to migrate from the existing Capital Expenditure (CAPEX) model to an Operating Expenditure (OPEX) model.
- Develop a plan to standup a redundant site to support HCHBNet services. Once the redundant site is operational, ongoing management and support of the redundant site will be part of Task 3.
- Implement new technologies/solution to comply with new Office of Management and Budget (OMB) mandates and other federally mandated requirements to address critical vulnerabilities. Gather requirements and provide technical support to ensure successful compliance with these new OMB mandates.
- Allow for future growth and implementation of new technology, as it becomes available, and recommend operational improvements and architectural changes.
- Refresh new desktops and laptops which are outside of the normal desktops/laptops replacement/refresh activities identified under Task 5: IT Service Desk Support. All equipment will be GFE.
- Note: Excluded are the cloud platforms, which DOC/OCIO will procure from another source or which the Contractor will purchase under the ODC Ancillary Products/Service CLIN.
- Note: Innovation environments within vendor's labs is permitted if on the vendor's time, equipment and funded by the vendor.

C.4.12 TASK 12 – AUDIO VISUAL AND VIDEO TELECONFERENCING (VTC) O & M SUPPORT

The contractor will provide support to ensure that the audio visual and video teleconferencing systems are operating at optimal level.

- Support daily VTC operational and maintenance activities to include conducting daily health check of VTC system and components. Respond to ticket assignments and provide resolution.

- Execute all aspects of videoconferencing including call setup, end user training, troubleshooting, and follow through on escalation of trouble incidents occurring during calls;
- Respond to client service desk calls for support, troubleshooting, or other requests covered under the client agreement;
- Perform VTC testing to include connectivity testing of local VTC units in the HCHB campus with remote VTC connections.
- Lead or assist in the support (hands-on if necessary) of special events, high profile senior executive meetings, town halls requiring videoconferencing as directed by the client;
- Provide technical consultation, support, and act as lead contact for all videoconferencing operations and maintenance;
- Solve all technical issues related to telepresence infrastructure and endpoints with minimal downtime;
- Setup WebEx sessions for remote users that are not able to participate in meetings via video conferencing
- Perform quarterly engineering analysis of requirements for videoconference support and provide recommendations of preferred solutions that optimize engineering, management, and cost parameters;
- Maintain usage statistics, issue and repair logs, or other collection/reporting systems;
- Create and modify user documentation and standard operation procedures. Review and update of the documentation shall be performed on an annual basis at minimum and with each major change to systems being managed.

C.4.13 TASK 13 - LIVE WEBCAST STREAMING SUPPORT (OPTIONAL)

- Provide Production Services to include:
  - Contractor must provide all personnel and equipment necessary to produce live webcasting events currently estimated at four events per year and have an understanding of audio/video formats and encoding processes. Production includes all meetings and preparations necessary to identify and set-up required resources (both government and contractor resources) prior to the event, support during event, recording and broadcast of event and wrap up, post-event.
  - Events must be 508 compliant and accessible
  - Inclusive in services is project management to oversee all pre-, event and post-event activities
  - Contractors must be capable of providing production services within the HCHB campus area only.
  - Contractors should be able to provide single- or multi-camera recording capability
- Provide Registration Services to include:
  The webcast portal will allow the government to customize the registration fields beyond the basic requirements (first name, last name, organization, email address, business phone number).
  - Customized registration confirmation, event updates, event reminders and thank you emails will be offered through the contractor's webcasting portal. The government

will have access to the webcasting portal or personnel to upload the preferred email communications. The government will provide details on timing of communications.

- Provide Broadcast Capability Services to include:
    - The contractor will provide a live webcasting portal website to support a maximum of up to 45,000 concurrent viewers. An estimated 4 events are to occur per year. The Contractor should have the live portal available at least 5 days before the event.
    - The webcasting portal will be made available via a personalized website link; will be offered in but not limited to Windows Media Player®, Adobe Flash® and RealPlayer® (or current popular media players); and will stream live from the Internet with no additional plug-ins.
    - The webcasted sessions shall support the minimum bit rate for delivery of quality sessions that can be viewed
    - The webcasting portal shall be viewable on a variety of desktop, laptop, smart phone and tablet devices and all popular browsers to include but not limited to (Internet Explorer, Chrome, Firefox, Safari, etc.)
    - The webcasting portal shall allow the presenter and/or government to upload presentations in Microsoft Office Suite of products to include but not limited to Microsoft PowerPoint, Word, Excel or PDF format
    - The webcasting portal will be customizable with government provided event branding and graphics, such as a web banner.

      Furthermore, the contractor shall provide a webcasting portal URL for the government to include on DOC websites that will be active during the event and for the duration of the archive period.
    - The webcasting portal will offer the viewers the ability to live chat with other viewers. Viewers will be able to conduct private chats with other viewers or chat in a community setting within the presentation portal.
    - Contractors must provide optional moderated audience Q&A capabilities during and live polling events
- Provide Archiving/File Formats Services to include:

  Post-event, contractor must provide archived versions of the event to the government in a format as required by the customer. Formats may include: DVD, Blue Ray, CD, USB or internet formats
    - Archived events on the webcasting portal and those delivered to the government must be transcribed so as to be 508-compliant. The following website provides information on Section 508 compliance: http://www.howto.gov/web-content/accessibility/508-compliant-and-accessible-multimedia.
- Provide Event Reporting Services to include:

  The webcasting portal shall capture and provide the following reports:
    - Registration statistics;
    - Number of viewers for each presentation;
    - The length of time each viewer views each presentation;
    - Total number of unique registered viewers for the entire webcasting event per day;
    - Archived presentation viewer data.
- Security Requirements: The Hosting site shall be FIPS compliant and support security of email transmittal if email transmittal is required as part of the service.

SECTION C – DESCRIPTION/SPECIFICATIONS/STATEMENT OF WORK

C.4.14 COOPERATION (ALL TASKS)

The success of this Task Order is largely dependent on the willingness and ability of the Contractor to cooperate fully with other stakeholders. The Contractor shall cooperate fully with OCIO, other DOC staff and contractors, and with staff and contractors at other DOC Operating Units; share information; openly discuss issues and concerns; and work towards the common resolution of issues and problems and accomplishment of DOC missions. Network and telecommunications support includes support service integration (e.g., integration of all the support tasks in this task order).

The Contractor's staff shall be fully instilled with the skills to provide excellent customer service and a high degree of cooperation with the Government and other support contractors.